

PTO/SB/08A (10-01)

Approved for use through 10/31/2002. OMB 0651-0031 ,

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of

Co	mplete if Known	DECE	14 (PP
Application Number	10/068,295	RECE	IVED
Filing Date	February 5, 2002		1
First Named Inventor	Mitchell, Oscar	DEC O	R 2002
Art Unit	2151		ן ניינ
Examiner Name		Tachaalaau	Contar 2100
Attorney Docket Number	501143.000019	Technology	reliter 2100

			U.S. PAT	ENT DOCUMENTS	
Examiner Initials	Cite No.1	Document Number Number - Kind Code ² (if known	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
<u> </u>	A1	us- 6,341,299	01-22-2002	Romain	
LC	A2	us- 6,157,955	12-05-2000	Narad et al	
10	A3	us- 6,151,393	11-21-2000	Jeong	
LU	A4	us- 6,141,705	10-31-2000	Anand et al	
ic	A5	us- 6,134,244	10-17-2000	Van Renesse et al	
Li	A6	us- 6,088,453	07-11-2000	Shimbo	
LV	A7	us- 5,987,574	11-16-1999	Paluch	
10	A8	us- 5,983,299	11-09-1999	Qureshi	
10	A9	us- 5,764,554	06-09-1998	Monier	
LL	A10	us- 5,724.279	0303-1998	Benaloh et al	
w	A11	us- 5,699,537	12-16-1997	Sharangpani et al	
u	A12	us- 5,542,061	07-30-1996	Omata	
il	A13	us- 4,799,149	01-17-1989	Wolf	
		US-			

	FOREIGN PATENT DOCUMENTS								
Examiner Initials		Foreign Patent Document Courby Code 3 - Number 4 - Kind Code 5 (# known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	Τ'			
						H			
						_			
				e angle is marked any her, <u>also provided and to page</u> of the or the second and the committee in committee in com-		-			
						_			
						-			

Examiner Date Signature Considered

Engish language transactions attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

^{*}EXAMINER: Initial if reference considered; whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08B (10-01) Approved for use through 10/31/2002. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of Information unless it contains a valid OMB

Substitute for form 1449B/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

of

Sheet 2

Complete if Known 10/068,295 **Application Number** February 5, 2002 Filing Date Mitchell, Oscar First Named Inventor 2151 Group Art Unit Examiner Name Attorney Docket Number 501143.000019

Center 2100

		OTHER PRIOR ART - NON PATENT LITERATURE DOCUMENTS	log
Examiner Initials	Cite No.1	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T2
re	C1	MENEZES, A.J., et al "Efficient Implementation" from theHandbook of Applied Cryptography, (Boca Raton, CRS Press, 1997), pp. 591-607.	
20	C2	DIMITROV, V. and COOKLEV, T., "Two Algorithms for Modular Exponentiation Using Nonstandard Arithmetics" IEICE Trans. Fundamentals, Vol. E78-A, No. 1, January 1995.	
ic	СЗ	KOC, C.K. and HUNG, C.Y., "Carry-Save Adders for Computing the Product AB Modulo N" Electronics Letters, Vol. 26, No. 13, (June 21, 1990), pp. 899-900	
LC	C4	FREKING, W. L. and PARHI, K.K., "Montgomery Modular Multiplication and Exponentiation in the Residue Number System" Proc. 33rd Asilomar Conf. Signals Systems and Computer, October 1999, pp. 1312-1316.	
ic	C5	TENCA, A.F. and KOC, C.K., "A Scalable Architecture for Montgomery Multiplication" in: KOC, C.K. and PAAR, C., Cryptographic Hardware and Embedded Systems, CHES 99, Lecture Notes in Computer Science, No. 1717. 1998, New York, NY: Springer-Verlog, 1999.	
Le	C6	KOC, C.K. and ACAR, T., " Montgomery Multiplication in GF (2k)" 3rd Annual Workshop on Selected Areas in Cryptography, (August 15-16, 1996), pp. 95-106.	
ic	C7	BAJARD, J.C., et al "An RNS Montgomery Modular Multiplication Algorithm" IEEE Transactions on Computer, Vol. 47, No. 7, (July 1998), pp. 766-776.	
Lc	C8	ELDRIDGE, S.E., "A Faster Modular Multiplication Algorithm" International Journal of Computer Math, Vol. 40, (1991), pp. 63-68.	
LC	С9	BOSSALAERS, A, et al "Comparison of Three Modular Reduction Functions" In Douglas R. Stinson, editor, Advances in Cryptology CRYPTO '93, Vol. 773 of Lecture Notes In Computer Science, (August 22-26, 1993), pp. 166-174.	
LC	C 10	MONTGOMERY, P.L., "Modular Multiplication Without Trial Division" Mathematics of Computation, Vol. 44, No. 170 (April 1985), pp. 519-521.	
W	C 11	KOC, C.K., et al "Analyzing and Comparing Montgomery Multiplication Algorithms" IEEE Micro, Vol. 16, Issue 3, (June 1996), pp. 26-33.	

Examiner		Date	121161	04
Signature	w w	Considered	14 4 01	

^{*}EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Tredemark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.



PTO/SB/08B (10-01)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO				Complete if Known RECEIVED Application Number 10/068,295					
				Application Number	10/068,295	ILOET .			
INFORMATION DISCLOSURE				Filing Date	February 5, 2002		•		
STATEMENT BY APPLICANT			PPI ICANT	First Named Inventor	Mitchell, Oscar	DEC 0 3 20			
			LIOAIII	Group Art Unit	2151		0400		
	(use as many shee	ets es	s necessary)	Examiner Name		abaalaay Cent	er 2100		
Sheet	3	of	3	Attorney Docket Number	2151 501143.000019 Te	Cilliology of			

		OTHER PRIOR ART NON PATENT LITERATURE DOCUMENTS	
Examiner Initials	Cite No. 1	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	т
Lu	C 12	KORNERUP, P., " High-Radix Modular Multiplication for Cryptosystems" Department of Mathematics and Computer Science, (1993), pp. 277-283.	
LC	C 13	SUNAR, B. and KOC, C.K., "An Efficient Optimal Normal Basis Type II Multiplier" Brief Contributions, IEEE Transactions on Computers, Vol. 50, No. 1, (January 2001), pp. 83-87.	
LC	C 14	KOC, C.K., "Comments on' Residue Arithmetic VLSI Array Architecture for Manipulator Pseudo-Inverse Jacobian Computation" Communications, IEEE Transactions on Robotics and Automation, Vol. 7, No. 5, (October 1991), pp. 715-716.	
LC	C 15	SAVAS, E. and KOC, C.K., "The Montgomery Modular Inverse-Revisited" IEEE Transactions on Computers, Vol. 49, No. 7, (July 2000), pp. 763-766.	
2	C 16	WALTER, C.D., "Montgomery's Multiplication Technique: How to Make it Smaller and Faster" in Cryptographic Hardware and Embedded Systems - CHAS 1999, C. Paar (Eds.). K. Ko, Ed. 1999, Springer, Berlin Germany, pp.61-72.	
LC	C 17	OH, H. and MOON, J., "Modular Multiplication Method" IEE ProcComput. Digit.Tech., Vol. 145, No. 4, (July 1998), pp. 317-318.	
LC	C 18	BLUM, T., "Modular Exponentiation on Reconfigurable Hardware" Master's thesis, ECE Department, Worcester Polytechnic Institute, Submitted to Faculty 1999-04-08, Published May 1999. Retrieved from the Internet <url: available="" blum.pdf="" etd="" etd-090399-090413="" http:="" pubs="" unrestricted="" www.wpi.edu="">.</url:>	
LC	C 19	MARWEDEL, P., et al. "Built in Chaining: Introducing Complex Components into Architectural Synthesis." April 1996. Proceedings of the ASP-DAC, 1997. [online]. Retrieved from the Internet <url: 1997="" aspacpdf="" aspdac="" eldorado.uni-dor="" f84="" forshung="" http:="" ls12="" mund.de:8080="">.</url:>	
H	C 20	TIOUNTCHIK, A., and TRICHINA, E., "RSA Acceleration with Field Programmable Gate Arrays" Lecture Notes in Computer Science, Vol. 1587, pp.164-176. Retrieved from the Internet: <url:http: 274658.html="" citeseer.nj.nec.com="">.</url:http:>	
		•	

Examiner	July -	Date	19/10/01
Signature	W	Considered	12116104

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

^{*}EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.